VANET 환경에서 오류수정부호를 사용한 V2I 인증 프로토콜

이수연*

요 약

VANET(Vechicular Ad-hoc Network)은 지능형 차량들로 이루어진 애드혹 네트워크 환경으로서 최근 들어 그 연구가 활발하게 진행되고 있는 분야이다. VANET은 원활한 교통 소통, 사고 방지 등 여러 가지 편리한 기능들을 제공하지만 그 기반을 애드혹 네트워크에 두고 있기 때문에 애드혹 망에서 발생하는 보안 문제를 가지고 있고 또한 그 환경적 특성에 따라 추가적인 보안 요구 사항이 존재한다. 본 논문에서는 오류수정부호(Error Correcting Code)의 생성행렬을 사용하여 부호화된 인증서를 생성하고 이를 기반으로 차량의 익명성과 비연결성을 제공하는 V2I(Vehicular to Interface) 인증 프로토콜을 제안한다. 또한 기존 방식에서 차량 등록 및 인증 서버(KDC)의 차량 비밀 키 관리에 대한 오버헤드 문제를 해결하게 되었다.

V2I Authentication Protocol using Error Correcting Code in VANET Environment

Suyoun Lee*

ABSTRACT

VANET(Vehicular Ad-hoc Network) is a kind of ad hoc networks consist of intelligence vehicular ad nodes, and has become a hot emerging research project in many field. It provide traffic safety, cooperative driving and etc. but has also some security problems that can be occurred in general ad hoc networks. Also, in VANET, vehicles should be able to authenticate each other to securely communicate with network-based infrastructure, and their locations and identifiers should not be exposed from the communication messages. This paper proposes V2I(Vehicular to Infrastructure) authentication protocol that anonymity and untraceability of vehicular using Error Correcting Code that generate encoding certification using generation matrix. The proposed scheme based on ECC resolves overhead problems of vehicular secure key management of KDC.

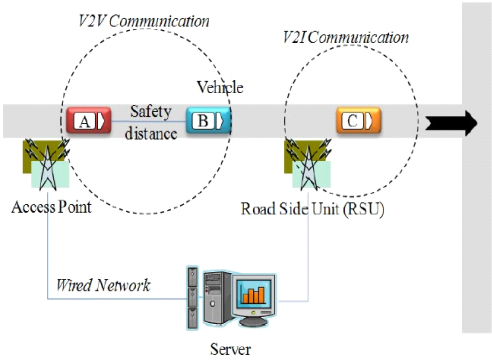
Key words : Error Correcting Code, VANET, authentication protocol

접수일(2011년 11월 18일), 수정일(1차: 2011년 12월 12일), 게재확정일(2011년 12월 20일)

* 백석문화대학 인터넷정보학부

1. 서 론

차량 애드혹 네트워크 (Vehicular Ad-hoc NETwork; VANET)는 MANET (Mobile Ad-hoc NETwork)의 한 형태로 다수의 차량이 무선통신을 이용하여 차량과 차량 (Vehicular to Vehicular: V2V) 또는 차량과 기지국(Vehicular to Interface: V2I)의 네트워킹을 자율적으로 형성하는 차세대 네트워킹 기술이다. VANET에서 제공되고 있는 차량 통신은 교통정보 제공 서비스, 인터넷 접속 서비스, 엔터테인먼트 서비스 등을 주목적으로 V2I통신이 활용되며 차량안전 관리 정보 교환, 교차로 진입 제어, 차량 주변의 상황을 고려한 실시간 서비스 등을 주목적으로 하는 V2V통신이 이용된다. V2I에서는 기존의 무선 환경에서 존재하는 보안 위협과 차량의 고속이동 및 네트워크 환경의 급격한 변화 때문에 발생하는 다양한 보안 위협이 존재한다. 뿐만 아니라 차량의 이동 정보가 쉽게 노출될 수 있는 문제점이 있어 개인의 프라이버시가 침해될 수 있다. 이를 해결하기 위해 기존에 많은 연구가 이루어졌고 익명 ID기반 집합 방식, 그룹서명 방식 등이 프라이버시 침해를 방지하기 위한 해법을 제시했다. 하지만 관련된 연구에서 제시된 기법은 프라이버시 침해를 방지하기 위해 신뢰기관의 키 저장 공간 및 차량의 계산량에 대한 오버헤드 등의 문제점을 갖고 있다 [1][2].



(그림 1) V2I 통신 환경

V2I환경에서 인증 프로토콜을 설계하기 위한 보안 요구사항 중 차량 개인의 프라이버시를 보장하고 효율적인 통신량과 저비용의 계산량이 가장 중요한 항목이다. 따라서 본 논문에서는 V2I환경에서 오류수정 부호의 대수적 특성을 이용하여 인증 프로토콜을 설계하였다. 제안된 인증 프로토콜은 프라이버시를 위한 익명성과 비연결성을 제공하고 저비용의 계산량을 유지하면서 신뢰 서버의 오버헤드로 알려진 차량의 비밀키 관리 문제를 해결하였다.

2. 관련 연구

2.1 프라이버시(Privacy)를 위한 보안요구사항

V2I통신에서 인증 프로토콜 설계 시 차량의 개인정보 즉 아이디, 위치 등과 같은 차량 개인의 프라이버시를 보호하기 위해 다음과 같은 사항은 만족해야 한다.

- 익명성(anonymity)

어떠한 차량의 아이디 정보도 네트워크 내부의 메시지로부터 노출되지 않아야한다. 이 성질은 아이디 노출로부터 사용자의 프라이버시 위협을 보호하기 위해 제공돼야하는 성질이다. 익명아이디를 사용함으로써 이 성질은 만족시킬 수 있다.

- 비연결성(stateless)

이웃 차량이나 신뢰 서버는 특정 메시지로부터 특정 차량의 이동경로를 파악할 수 없어야한다. 비연결성은 사용자의 위치에 대한 프라이버시를 제공하기 위한 성질이다. 익명 아이디를 주기적으로 변경해줌으로써 이 성질을 만족시킬 수 있다.

차량의 프라이버시를 보호하기 위한 관련 연구는 익명 ID기반 집합방식과 그룹서명 방식으로 분류된다. 관련 연구에 대한 설명은 다음과 같다.

2.2 익명 ID기반 집합 방식

VANET에 참여하는 차량이 신뢰기관으로부터 익명 ID집합과 그에 따른 개인키 및 인증서의 집합을 부여받아 사용하는 방법을 제안하고 있다. 이들 방법

에서 차량은 익명ID를 이용해 익명성을 보장받고 그에 따른 개인키로 메시지의 인증 문제를 해결한다. 차량은 익명ID를 메시지마다 갱신하여 사용하고 소진 시 다시 신뢰기관에 접속하여 새로운 집합을 부여받는다.

Raya와 Hubaux는 다량의 익명인증서를 사용하는 시스템을 제안하였다 [3]. 각 차량은 초기에 다량의 익명 인증서와 인증기관의 인증서가 설치 된 상태이며 주기적으로 다량의 익명인증서를 발급받아 교체해야한다. 따라서 차량에 많은 저장 공간이 요구되며 일반 인증서 철회 방법을 사용할 경우에는 CRL (Certificate Revocation List) 크기가 매우 커지는 문제점을 지니고 있다. 따라서 인증서 철회방식에 대한 여러 가지 해결책이 필요하다.

2.3 그룹 서명 방식

사용자 각자의 그룹 서명키와 그룹이 갖는 하나의 그룹 공개키를 이용하여 메시지에 대한 서명 및 확인을 할 수 있는 기법으로 익명성을 보장하면서 서명을 확인할 수 있다는 장점을 갖는다. Lin 등 [4]은 Boneh 등의 그룹서명 [11]과 신원기반 공개키 시스템을 활용한 시스템을 제안하였다. 이 시스템은 차량 간 통신은 그룹서명을 사용하고 RSU가 차량에 메시지를 전달할 때에는 일반 신원기반서명기법을 사용하고 있다. 이 방식은 익명 ID기반과 마찬가지로 철회 목록을 각 차량에게 전달하여 철회하는 형태를 VANET에서 사용하기에는 적절하지 못하며 이 서명기법은 영지식 기술을 이용하는 서명이므로 서명자체가 효율적이지 못하다.

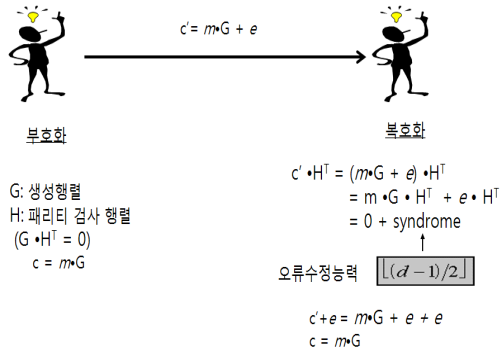
Calandriello 등 [1]도 Lin과 마찬가지고 그룹서명기법을 사용하지만 그룹서명을 사용하여 메시지를 교환하는 것이 아니라 각 차량은 그룹 서명키를 이용하여 익명인증서를 스스로 만들어 사용하는 방법을 제안한다. 자체적으로 불연결성을 제공하는 익명의 공개키 쌍을 지속적으로 생성하여 사용할 수 있다는 장점을 지니고 있지만 생성된 익명인증서를 사용하기 위해서는 인증서를 사용하기 위해 그룹서명을 확인해야하고 익명인증서를 이용하여 서명된 메시지를 확인해야한다. 따라서 각 메시지를 확인하기 위한 비용이 비교적 크다.

3. 개선 된 V2I 인증 프로토콜

본 장에서는 오류수정부호의 대수적인 구조를 이용하여 차량의 익명성을 함께 제공하는 인증방식을 제안한다. 제안한 프로토콜은 대칭키 암호화 방식으로 저비용의 계산량을 유지하면서 차량 등록 및 인증 서버 (KDC)의 키 관리 문제는 각 차량의 부호화 된 인증서 발급을 통하여 해결된다.

3.1 오류수정부호(Error Collecting Code)

오류수정부호는 잡음에 의해서 유도되는 채널오류가 존재하는 통신망 내에서 신뢰성 있는 통신을 위하여 사용되어진다. 암호학에 적용된 오류수정부호의 응용은 McEliece [5]에 의해 처음 소개되었다. 이것은 Berlekamp, McEliece, van Tilborg [6]에 의해 제시된 선형블록코드의 일반적인 복호화 문제는 NP-complete라는 초기 논문의 결과이다. 선형블록코드의 원리는 다음과 같다. 길이가 N, 차원이 K 그리고, 최소거리가 D인 선형 오류수정부호는 (N, K, D)로 표기되어진다. 예를 들어 (7,4) 선형블록코드인 경우 4개의 메시지 순열 (Sequence)에 3개의 패리티 검사 비트 (Parity check bit)를 추가하여 7비트의 코드워드를 생성하는 것이다. 이진 k-tuple의 메시지 m은 $c = m \cdot G$에 의해 N 비트의 코드워드로 부호화되어진다. 여기서, G (Generator matrix)는 $K \cdot N$의 생성행렬이다. 오류벡터 e가 c에 추가되어 $c' = c + e$ 벡터를 얻는다. 만약, e의 해밍 가중치가 $c = \lfloor (D-1)/2 \rfloor$ 보다 작거나 같다면 c'는 신드롬 벡터 $s = c' \cdot H^T$를 사용하여 c로 복호화 될 수 있다. 여기서, H (Parity check matrix)는 $G \cdot H^T = 0$이 되는 $(N-K) \cdot N$ 패리티 검사행렬이다. 여기서, H^T는 H의 역행렬이다. (그림 2)는 오류수정부호를 사용한 부호화와 복호화 과정을 나타낸다.



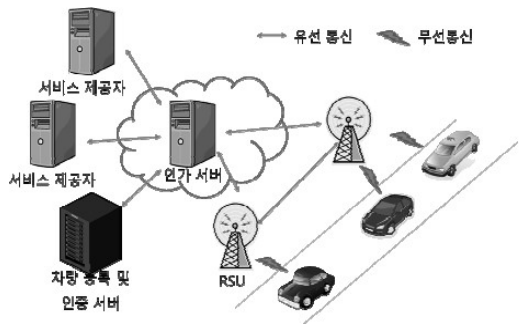
(그림 2) 오류수정부호를 사용한 부호화/복호화 과정

3.2 오류수정부호를 이용한 인증 프로토콜

(그림 3)과 같이 차량등록 및 인증서버, 다수의 차량, 도로에 설치된 RSU 그리고 인가 서버의 참여를 가정한다.

• 인가 서버 (AS: Authorization Server)

신뢰 기관에서 관리하는 서버로서 RSU를 관리하고 차량 등록 및 인증 서버를 이용하여 차량의 통신 인가를 한다. RSU, 차량 등록 및 인증 서버와 유선으로 연결되어 있고 각 대칭키를 공유하고 있다.



(그림 3) 시스템 환경

• RSU (RoadSide Unit)

차량의 통신을 돕기 위한 통신 설비로 도로에 일정한 간격으로 고정되어 있다. 인가 서버와 유선으로 연결되고 대칭키를 공유하고 있다.

• 차량

OBU를 이용하여 무선 통신을 하고 안전한 저장장치(tamper-proof device)를 가지고 있다.

• 차량 등록 및 인증 서버 (KDC)

차량이 판매되면 고유한 아이디와 마스터 키를 부여하고 차량 내부의 안전한 저장장치에 이를 저장한다. 인가 서버와 유선으로 연결되어 있고 대칭키를 공유한다.

3.2.1 시스템 가정

차량 간 통신과 차량에서 RSU간 통신은 프라이버시가 보장되어야 하지만 RSU에서 차량 간 통신은 프라이버시가 요구되지 않으므로 기존 보안 메커니즘을 사용하여도 무관하다. 따라서 본 논문에서는 V2I 통신 중 단일 홉 방송 메시지에 초점을 맞추고 있다. 이 논문은 다음과 같은 내용을 가정한다.

- 차량 노드들은 VANET 환경에 참여하기 전에 차량 등록 및 인증 서버에 신원을 등록하고 익명 ID와 인증서(c)를 지급받는다.
- 차량 등록 및 인증 서버는 신뢰할 수 있는 기관으로 안전하다고 가정한다.

3.2.2 표기법

- KDC : 차량 등록 및 인증 서버
- V : 차량
- K_{KDC} : 차량 등록 및 인증 서버 개인 키
- k : 차량의 개인 키
- $E_k(M)$: 대칭키 암호화함수
- $D_k(M)$: 대칭키 복호화함수
- kek : 키 암호화용 키, 차량과 RSU 사이에 공유된 세션 키를 설립하기 위해 사용
- r : 임의의 난수
- t : 해밍 가중치
- c : 코드워드
- G : 생성 행렬
- H : 패리티 검사 행렬
- id : 차량의 신원

• h : 키를 이용하는 해쉬 함수
• e : 오류벡터
• $f()$: 대칭형 암호 알고리즘

3.3.3 사전단계

Berlekamp-Massey 알고리즘 [7,8]이나 일반적인 Euclidean 알고리즘과 같은 효율적인 복호화 알고리즘을 이용 할 수 있는 이진(N, K, D)선형블록코드를 생성한 후 차량 등록 및 인증 서버는 자신만이 알고 있는 패리티 검사행렬 H와 함께 $K \bullet N$ 비체계적 (Non-systematic) 생성행렬 G를 만든다. 부호는 $c = \lfloor (D-1)/2 \rfloor$ 이하의 오류를 수정 할 수 있게 설계된다.

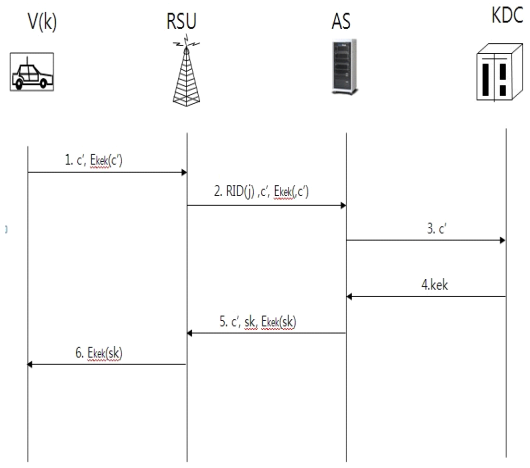
3.3.4 차량 등록 단계

차량이 출고되면 차량은 차량 등록 및 인증 서버에 등록한다. 차량이 등록되면 차량 등록 및 인증 서버는 차량에게 아이디와 마스터 키, 그리고 부호화된 인증서 $c = m \bullet G$ 를 차량의 안전한 장치에 저장한다. $m = f(k_{KDC}, [id, k])$

3.3.5 익명의 차량 인증 단계

차량이 도로를 이용하면서 도로에 설치된 RSU와 인증을 하여 서비스 제공자 서버로부터 콘텐츠를 제공받아서 이용하는 단계이다. 차량 등록 및 인증 서버는 임의의 값 (r)을 주기적으로 방송한다.

단계 1: V는 KDC가 주기적으로 방송한 r과 자신의 id를 이용하여 $x = h(k, [r, id])$를 계산하고 이후 아래 [알고리즘 1]에 따라서 x를 오류벡터 e로 변형한다. V는 순서보존 (order preserving) 사상을 사용하여 s비트의 해쉬값 $h(k, [r, id])$를 길이 N, 해밍가중치 $c = \lfloor (D-1)/2 \rfloor$ 인 오류벡터 e로 변형시키고 이 오류벡터 e를 추가한 부호화된 비밀 키 인증서 $c' = m \bullet G + e$와 $E_{kek}(c')$를 RSU에게 보낸다. (해밍가중치가 t인 오류벡터의 수는 $\binom{N}{t}$)



(그림 4) V2I 인증 프로토콜

- 만일 오류벡터의 집합과 정수 간에 일대일 대응이 존재한다면 이러한 오류벡터들은 추가의 정보를 전달하기 위해 사용되어질 수 있다.
- 만일 s가 $\lfloor \log_2 \binom{N}{t} \rfloor$ 이하이면 s비트의 해쉬값 $h(k, [r, id])$은 0과 $\binom{N}{t}$ 사이의 정수 x로 간주될 수 있으며, 벡터의 사전적인 순서 (lexicographic order)와 정수의 자연적인 순서 (natural order)로 정의된 순서보존 사상에 의하여 길이가 N이고 해밍 가중치가 t인 오류벡터 e로 사상될 수 있다.
- s가 $\lfloor \log_2 \binom{N}{t} \rfloor$ 보다 큰 경우에는 s -비트 해쉬값의 오른쪽 s- $\lfloor \log_2 \binom{N}{t} \rfloor$ 비트가 $h(k, [r, id])$를 형성한다.

[알고리즘 1] : 정수 x를 해밍가중치 t의 이진 오류벡터 $e = (e_1, e_2, \ldots, e_N)$로 변화시키는 알고리즘이다.

If $s \le \lfloor \log_2 \binom{N}{t} \rfloor$ then $x \leftarrow h(k, [r, id])$ else $x \leftarrow h(k, [r, id])$;
for i = 1, 2, . . . , N {
if $x \ge \binom{N-i}{t}$ then {$e \leftarrow 1$; $x - \binom{N-i}{t-1}$;
$t \leftarrow t-1$; }
else $e_i \leftarrow 0$;

단계 2: V에게 메시지를 받은 RSU는 자신의 아이디 $RID(j)$와 V에게 받은 메시지 c'와 $E_{kek}(c')$를 인가 서버 AS에게 전송한다.

단계 3: RSU에게 $RID(j)$, c'와 $E_{kek}(c')$를 전달 받은 AS는 저장 받은 내용을 저장하고 c'를 KDC에게 전송한다.

단계 4: AS에게 c'를 전달 받은 KDC는 c'가 등록 된 차량인지를 확인한다. 즉, 복호화 과정을 수행하고 m과 오류벡터 e를 분리한다. 복호화 과정은 식 1)과 같다. ($G \cdot H^T = 0$)

$$c' \cdot H^T = (m \cdot G + e) \cdot H^T \qquad \text{식 1)}$$

V의 실제 신분 id와 대응되는 비밀키 k는 $m = f(k_{KDC}, [id,k])$를 KDC로 복호화하여 얻을 수 있다. 이제, KDC가 V의 신분을 확인하면 합법적인 차량 등록자로 간주되어진다. 그 후 s비트의 해쉬 값 $h(k,[r,id])$는 KDC에 의해 계산된다.

[알고리즘 2] : 해밍가중치가 t인 이진 오류벡터 e = (e1, e2, . . . , eN)를 $0 \le x < \binom{N}{t}$인 정수 x로 변형시켜준다.

$x = 0$
for i = 1, 2, . . . , N {
if e_i =1 then { $x \leftarrow x + \binom{N-i}{t}$; $t \leftarrow t-1$}

만일 계산된 s-비트 해쉬 값이 e로부터 유도된 x와 같다면 KDC는 V를 인증한다. s가 $\lfloor \log2(\binom{N}{t}) \rfloor$보다 큰 경우는 s 비트 해쉬 값의 왼쪽 $\lfloor \log2(\binom{N}{t}) \rfloor$비트가 x와 비교한다. KDC가 차량을 인증하게 되면 kek를 AS에게 전송하고 자신의 데이터베이스에 저장되어 있는 c와 kek를 대체한다.

단계 5: KDC에게 kek를 전달받은 AS는 kek를 이용하여 $D_{kek}(c')$를 통해 c'가 존재하는지 확인한다. 존재한다면 임의의 sk를 선택하고 $E_{kek}(sk)$를 계산한다. 이후 RSU에게 c', sk, $E_{kek}(sk)$를 전송한다.

단계 6: AS에게 c', sk, $E_{kek}(sk)$를 전송받은 RSU는 c',sk를 저장하고 차량에게 $E_{kek}(sk)$를 전송한다.

단계 7: RSU에게 $E_{kek}(sk)$를 전달받은 V는 kek를 이용하여 sk를 계산한다. V는 sk를 알게된다. V와 RSU 사이에 세션 키 sk가 공유되므로 공유된 키를 이용하여 데이터를 암호화하여 전송한다.

3.3 개선 된 V2I 인증 프로토콜 분석 및 평가

3.3.1 프라이버시 보호

• 익명성 제공

KDC를 가진 차량 등록 및 인증 서버만이 차량의 키와 신분을 식별할 수 있다. $m = f(k_{KDC}, [id,k])$는 차량 등록 및 인증 서버로부터 차량의 비밀 키 관리 문제를 해결하고 차량의 익명성을 제공한다.

• 비연결성 제공

오류수정부호의 사용은 코드의 오류수정 능력을 이용하여 하나의 메시지 내에 비연결성을 포함한 차량 인증을 제공한다. 즉, $m \cdot G + e$ 처럼 부호화 된 인증서에 추가된 오류벡터는 차량 등록 및 인증 서버에게 차량에 대한 추가적인 정보를 보내는 것이다. 이 같은 목적을 달성하기 위해 차량 등록 및 인증 서버로부터 보내진 난수 r에 대한 응답 $h(k,[r,id])$는 순서보존 사상을 통해 오류벡터로 변형되어져 인증 시마다 변경이 되기 때문에 다른 차량이나 RSU가 알 수 없다.

3.3.2 효율성

해쉬 함수와 순서보전 사상을 사용하여 c'를 만들기 때문에 c'와 kek를 생성하는 데 걸리는 시간은 매우 짧다. 또한 암호화 방식도 대칭키 암호화 방식만 사용하기 때문에 암복호화에 걸리는 시간이 매우 짧다. 또한, 비밀 키 인증서는 차량 등록 및 인증 서버

가 차량의 비밀 키를 저장한 데이터베이스를 안전하게 유지할 필요가 없다.

3.4 비교 분석

[표 1]은 인증 프로토콜을 비교 분석한 결과이다. 익명 ID기반과 그룹서명방식에서는 연산량과 차량 등록 및 인증서버의 저장량 측면에서 제안한 방식이 더 효율적임을 보여주고 있다.

[표 1] 기존 프로토콜과 비교

구분	익명ID기반		그룹서명방식		제안방식	
	V	KDC	V	KDC	V	KDC
연산량	1・s	n・s	(n-1)s	1p+s	1・h+1・s	1s+1h+b
KDC 저장량	n・m		g・n		g・b	

공개키 연산: p, 비밀키 연산: s, 해쉬 연산: h, 유니캐스트: c, 브로드캐스트: b, 메시지 수: n, m: 등록된 차량 수, 그룹: g

4. 결 론

본 논문에서는 VANET 환경에서 차량의 프라이버시를 보호하기 위해 오류수정부호의 대수적 특성을 사용하여 차량의 익명성과 비연결성을 제공하는 개선된 인증 프로토콜을 제안하였다. 특히, 기존의 익명 ID기반과 그룹서명방식에서 저사양 차량의 연산량을 고려하지 않는 문제점을 연산량을 줄이므로 해결하였다 . 또한, 차량 등록 및 인증 서버가 차량의 비밀 키를 보관해야하는 저장 공간 문제를 해결하는 측면에서 기존 방식과 비교하여 제안된 인증 프로토콜의 효율성을 입증하였다. 향후에는 시뮬레이션을 통해 기존 연구 기법과 비교・분석을 연구할 계획이다.

참고문헌

[1] G. Calandriello, P. Papadimitratos and J. P. Hubaux, "Efficient and Robust Pseudonymous Authentication in VANET, " In Proc. International Workshop VANET, pp.19-28, 2007.

[2] J. Zhang, L. Ma, W. Su, and Y. Wang, "Privacy-Preserving Authentication Based on Short Group Signature in Vehicular Networks," Proceedings of the First International Symposium on Data, Privacy, and E-Commerce, pp. 138-142,

[3] M..raya and J.Hubaux, "Securing vehicular ad hoc networks," J. of Computer Security, vol. 15, no. 1, pp. 39-68, Jan.2007

[4] X. Lin, X. Sun, P,-H, Ho and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for Vehicular Coomunications", IEEE Trans, on Vehicular Technology, vol, 56, no.6, pp.3442-3456, 2007.

[5] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, " On the Inherent Intractability of Certain Coding Problems," IEEE Trans. on Inform. Theory, vol. 24, no.3, May. 1978, pp. 384-386.

[6] G. L. Feng and K. K. Tzeng, "A Generalized Euclidean Algorithm for Multisequence Shift-Register Synthesis, " IEEE Trans. on Inform. Theory, vol. 35, no. 3, May 1989, pp. 584-594

[7] D. Davis and R. Swick, "Network Security via private-key certificates", Operating System Review, vol.24, 1990, pp. 64-67.

[8] ETSI-GSM, Technical Specification GSM 03.20, " Security Related Network Functions," version 3.3.2, 1992.

[9] F.J.MacWilliams and N.J.A.Sloane, The Theory of Error-correcting Codes, North-Holland Publishing Company, 1977.

[10] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, "AMOEBA : Robust Location Privacy Scheme for VANET", IEEE Journal on Selected Areas in Communications 2007.

[11] D.Boneh, X.Boyen, and H.Shacham, "Short group signatures," Advaces in Crytpology, Crypto 2004, LNCS 3027, pp. 41-55, 2004

[저 자 소 개]

이 수 연 (Suyoun Lee)

1990년 단국대학교 전자계산학과 (이학사)

1993년 단국대학교 전산통계학과 대학원 석사(이학석사)

2003년 성균관대학교 전기전자 및 컴퓨터공학부 대학원 박사 (공학박사)

1997년 3월 ~ 현재 백석문화대학 인터넷정보학부 교수

email : sylee@bscu.ac.kr